Governor’s Office for Technology

Security Guidelines

January 8, 2001

Governor's Office for Technology
Security Guidelines

The following document is presented to serve as guidelines to assist the Commonwealth of Kentucky in addressing security issues. Many of these guidelines were primarily developed as lessons learned from previous security audits/assessments performed on the Governor's Office for Technology (GOT). You will notice that many of the guidelines listed below are not technology items but are procedural issues in nature. These have been included because many security issues are not about technology, but instead they are about "using" technology. Often what seems to be "common sense" procedures are not being followed due to various reasons such as lack of staff; lack of effective communication practices, etc.

Security considerations have been grouped into 10 categories as follows:
(1) Security Policy
(2) Security Organization
(3) Assets Classification and Control
(4) Personnel Security
(5) Physical and Environmental Security
(6) Communications and Operations Management
(7) System Access Control
(8) Systems Development and Maintenance
(9) Business Continuity Planning/Disaster Recovery
(10) Compliance

Lessons learned or recommended practices for each area have been included so that agencies will be more aware of security issues and assist agencies in protecting their information resources. This document is intended to be an on-going document that will be updated as needed.

Security Policy

- An agency should have documented information security policies available to all employees. Policies should define what you consider valuable and should specify what steps should be taken to safeguard those assets. GOT has developed a security policy and procedure manual to be implemented in the next 30 days. Also, available,

Security Organization

- A management framework should be established to initiate and control the implementation of information security. Ensure that your agency has designated an individual responsible for security. GOT has requested that each cabinet identify a security contact to serve as the focal point for all security communication and policy information from GOT.

Assets Classification and Control

- To maintain appropriate protection of assets, all major information assets should be accounted for and have an owner. An information asset inventory should be performed to identify the various items needed to protect your agency. Information such as the following should be defined: type of hardware, software, data; critical application systems; designated owner of information; physical or logical location, inventory item number; service levels, warranties, key contacts, etc. The Division of Asset Management is tasked with developing a system to track all assets within GOT.

- To ensure information assets receive an appropriate level of protection, security classifications should be used to indicate the need and priorities for security protection. Classification guidelines should be established. Categories such as sensitive, confidential, private or public may be considered.

Personnel Security

- Security should be addressed at the recruitment stage, included in job descriptions and contracts, and monitored during employment. Employees/contractors should sign confidentiality agreements. Also, employees/contractors should sign statements acknowledging their responsibility for security, adherence to policies and procedures, and also that Commonwealth resources are to be used for state business. GOT is in the process of modifying existing forms and will ensure that all current employees/contractors have signed such a form. These forms can be made available if desired.

- A process should be established to ensure that as employees and contractors are terminated/transferred/retired that security access is terminated immediately. The security area should be the focal point of this process. They should be notified

- Information security education and training should be developed for on-going employees. Ensure that staff attend on-going security training. GOT staff are attending security conferences and training on a regular basis.

- Security awareness program should be developed. This will increase awareness of security issues and also convey that management is serious about security. A security web portal is currently being designed that will increase security awareness among the enterprise.

- To minimize the damage from security incidents, and to monitor and learn from them, incidents affecting security should be reported through management channels as quickly as possible. Develop a security incident reporting policy and ensure that staff are knowledgeable of the process. Ensure appropriate follow up of security incidents. GOT has recently developed an internal security incident reporting form and policy that can be made available. In the immediate future, GOT will be requesting each cabinet to provide GOT a copy of their internal cabinet security incident reporting policy.

Physical and Environmental Security

- To prevent unauthorized access, damage and interference to the business normal course, all facilities supporting critical or sensitive business activities should be housed in secure areas.

- Identify physical entry controls.

- Formal badge access controls should be developed for secure areas.

- Removal of property from physical buildings should be controlled. Checkout procedures should be employed so that management is aware of property/assets leaving the physical facility.

- To prevent loss, damage or compromise of asset and interruption or business activities, equipment should be physically protected. Equipment location, power supplies, cabling, maintenance should all be considered.

- Ensure that data is properly removed from all equipment before disposal; i.e., policy for erasure of data from hard disk.

- Operating procedures should be documented.

- Incident handling procedures should be documented. These procedures include internal procedures for responding to security incident reports.

- Ensure segregation of duties; i.e., separation of development and operational facilities.

- Configure hardware to meet your security policy where applicable.

- Establish a procedure to review security hot fixes and services packs to determine if they should be applied to each server. The procedure should include a process to keep track of all system changes made to each server. A hard copy should be maintained.

- All security hot fixes available at server software installation should be applied.

- Microsoft hard disks should be formatted to NTFS.

- *Review all default settings before installation; particularly those default settings related to Microsoft*. Default settings rarely take security into consideration. Each setting should be reviewed based on the specific business requirements.

- Install minimal services required. Only the ports required for the server and/or application to function appropriately should be open. Remove or disable Web server services not required; disable FTP if it is not used.

- Ensure logs are enabled. As with any business system, there is a need to recreate and trace all activity. As data passes back and forth between tiers, the audit trail is easily obscured.

- GOT should periodically execute network mapping and scanning tools to understand what intruders who use such tools can learn about the GOT network and systems Execute vulnerability scanning tools on all systems to check for the presence of known vulnerabilities.

- To minimize the risk of systems failures, advance planning and preparation are required to ensure availability of adequate capacity and resources.

updates are made available. (GOT is finding that most viruses are detected at the exchange server due to virus updates not being applied to workstations.) Also, ensure virus protection procedures are in place for laptops.

- To maintain the integrity and availability of IT services, administrative functions such as back up of data, logging of events, environment monitoring are required. Ensure that logs are kept and maintained in accordance with KDLA or federal requirements.

- Set NT audit functions to the following:

NT Audit Policy

	Success	**Failure**
Logon and Logoff	X	X
File and Object Access		X
Use of User Rights		X
User and Group Management	X	X
Security Policy Changes	X	X
Restart, Shutdown and System	X	X
Process Tracking		

- Consider hiding servers from browser list when appropriate.

.

- Ensure that appropriate network controls are in effect. Consider using firewalls and intrusion detection devices. Internet firewall provides little protection. If sensitive data is being maintained, application firewalls should be used. Application firewall rules should be reviewed to ensure that only needed traffic is allowed. Network intrusion detection tools and host based intrusion detection tools may be needed. GOT is in the process of establishing a contract for intrusion detection tools.

- Computer media should be controlled and physically protected. There should be procedures for removable computer media and disposal of media.

- Encryption of sensitive information across the internet is essential. Ensure that user id and password are encrypted.

- There should be formal procedures to control allocation of access rights to IT services. There should be a procedure for requesting new user ids. In addition, there should be a regular review of user access rights to ensure that access is still valid.

- To prevent unauthorized user access, the cooperation of authorized users is essential for effective security. Users need to understand their responsibility. Effective password use according to password policy should be adhered to. Unattended user equipment should be closed down or password locks turned on.

- To ensure that connected users or computer services do not compromise the security of any other networked services, connections to networked services should be controlled. Dial in and modems provide back door connections that need to be closed. GOT will be issuing a forthcoming policy on this.

- To prevent unauthorized access to information held in computer systems, logical access control should be used to control access to applications and data. Application security provides another level of security.

- The use of individual account access rather than group user ids and passwords is encouraged for auditing purposes. Identification of group accounts and justification should be reviewed.

- Use of system administrator and database administrator privileges should be regularly audited.

- Non-expiring passwords should be not be used unless justification is appropriate.

- All default guest accounts should be renamed to a non-descriptive name. Review guest accounts and remove if appropriate.

- Rename the administrator account to a non-descriptive name. Consider removing the rights of this account and create a new local account with all rights.

- Grant local administrative rights to users through membership in local admin group.

- To detect unauthorized activities, systems should be monitored to ensure conformity to access policy and standards.

- Remove all administrative shares. Manually create those needed for applications.

- Restrict anonymous network access. Remove net shares; access to shares should only be based on a need to know.

- Minimize the number of users and groups on the server ; keep groups small.

- Set a very strong password for administrative accounts. Set up a procedure to routinely scan the administrator passwords.

- Accounts should be removed or disabled after a certain period of inactivity.

Systems Development and Maintenance

- To ensure that security is built into IT systems and applications, security requirements should be identified and agreed prior to development. Ensure that security language is addressed in all development contracts including Strategic Alliance Services (SAS) contracts.   Ensure that security architecture is outlined as a deliverable in the contract.

- To prevent loss, modification or misuse of user data in applications, appropriate security controls, including audit trails should be designed and implemented.   (Input data validation, internal processing validation, output data validation, data encryption, digital signatures, message authentication, non-repudiations, key management).

- Access to operational system files should be controlled. Developers should not have access to production.

- To maintain the security of application system software and data, project and support environments should be strictly controlled; (change control procedures, technical review of system changes; restrictions on changes to software).

- Developers should be aware of any known security vulnerabilities with the specific technology being proposed for the system. If known security vulnerabilities exist with the proposed technology platform, a plan should be developed to minimize or remove these vulnerabilities.

Business Continuity Planning/Disaster Recovery

- To counteract interruptions of business activities, business continuity plans should be supported servers.   This plan will include recovery for the network, critical enterprise applications, and utility applications such as email.

Compliance

- Ensure compliance with legal requirements. This may include statutory, regulatory or contractual requirements.

- Ensure compliance with software licenses. Asset inventory should be maintained to house software license information.

- To ensure compliance with organizational security policies and standards, the security of IT systems should be regularly reviewed and checked.

- Ensure that adequate reporting mechanisms are in place so security can be reviewed on a regular basis.

- Regular audits of operational systems should be conducted. To minimize interference to/from the system audit process, there should be controls to safeguard operational systems during system audits.

.